Research, Engineering and Development Advisory Committee (REDAC)

Meeting Minutes

January 16, 2002

On January 16, 2002, the Federal Aviation Administration's (FAA) Research, Engineering and Development Advisory Committee (REDAC) held a special meeting at the Holiday Inn Rosslyn, Westpark Hotel in Arlington, Virginia. Attachments 1 and 2 provide the meeting agenda and attendance, respectively.

Welcome and Introductory Remarks

Dr. Herman Rediess, Executive Director and Designated Federal Official of the Committee, read the public meeting announcement. Dr. Rediess reminded the Committee and audience that the meeting was an open to the public. As such, classified discussions would not take place. However, if Dr. Lyle Malotky, the Designated Federal Official of the Security Subcommittee and the Chair, Dr. Deborah Boehm-Davis, determine the discussion was moving to a classified level, the discussion would have to continue in a closed session at a later date.

Steve Zaidman Comments

Mr. Steve Zaidman, Associate Administrator of Research and Acquisitions, welcomed Admiral Paul Busick, FAA's Associate Administrator for Aviation Security, to the meeting. Mr. Zaidman discussed details about the transition of the FAA's security research to the Transportation Security Administration (TSA) under the auspices of the Department of Transportation (DOT). The Aviation and Transportation Security Act (ATSA) authorized \$50M a year for each fiscal year 2002 through 2006 for security research and development. Another \$20M will be transferred to the TSA from the Department of Defense's (DOD) Defense Advanced Research Projects Agency (DARPA). Mr. Zaidman also related upcoming deadlines in the ATSA law: January 18th screening of all carry-on bags on aircraft; February 17th awarding of security R&D grants, and an end of calendar year 2002 target date to have electronic detection systems (EDS) in place at major airports. Mr. Zaidman further announced that the ATSA established a Scientific Advisory Panel and an R&D Manager. The FAA Administrator will review the panel's composition. The R&D Manager will be required to submit an annual report on security technologies to the REDAC.

A discussion ensued on details relating to the makeup of the TSA. In addition, the REDAC members talked about the imperatives of better connectivity between the FAA, NASA, DOD, and the Scientific Advisory Panel as related to aviation security research and development.

Security Subcommittee Report

Mr. John Klinkenberg, Chairman of the Security Subcommittee, briefed the REDAC on the Aviation Security Technology Assessment. This effort, directed by the FAA Administrator in response to the events of September 11, 2001, reviewed over 1,300 suggestions from the public and industry to recommend courses of action. An initial meeting took place on October 25, 2001 with a follow-on meeting on November 16. A draft report was sent to FAA Administrator Garvey on November 20, and she was briefed on November 26. Among the Security Subcommittee's conclusions were:

- To approach security as a system;
- That there are no "silver bullets";
- To harden the cockpit door;
- To focus resources on unknown passengers;
- To demonstrate technology that can successfully screen people;
- That technology and human factors need improvement; and
- That automated flight is not acceptable.

Discussion on Security Report

Following Mr. Klinkenberg's presentation, there was a discussion of the Security Subcommittee Report. Key areas of discussion were:

- The importance of a distinction being made from the Rapid Response Team concerning intrusion-resistant doors versus ballistic-resistant cockpit doors. This team had strongly recommended intrusion-resistant and suggested further study on ballistic-resistant cockpit doors.
- The need to study some of the threats from a general aviation and cargo transport airline perspective.
- The importance of having a total "threat assessment." An assessment must be made before research can actually begin. The national threat assessment would be a combined effort of the appropriate security professionals such as the TSA, the DOD, the CIA, the FBI, etc. That effort would include a prioritization of threat assessment and the capital needed to spend on the highest probability of threat. Dr. Susan Hallowell related that a total systems architecture document had been developed that governs R&D based upon the threat. That architecture would be adjusted as the mission is expanded to work for the Transportation Security Administration. The term "threat assessment" should be stated as an "overall vulnerability analysis," which takes into account system-wide vulnerability and facility-specific threats.
- That wording in the report should reflect that automated flight or airspace denial systems are not feasible at this time and not for the foreseeable future and we do not recommend investment in those programs at this time.

Mr. Paul Hudson, Executive Director for the Aviation Consumer Action Project (ACAP), and a member of the Ad Hoc Security Subcommittee, provided alternative comments to the report. (Attachment 3)

The comments/suggestions made by the REDAC members would be incorporated into the draft report. The final draft would be transmitted to the members via email for final approval.

Committee Approval on FY 2004 Guidance

The Committee reviewed and offered suggestions to the letter from the REDAC to FAA Administrator, Jane Garvey. Among the suggestions were:

- To shorten the letter with bulleted items;
- Emphasize bigger issues such as systems engineering and tech transfer;
- Highlight structural issues regarding the Performance Based Organization;
- Include different issues associated with noise; and
- More specificity in the language concerning focused interaction with the FAA's Associate Administrators to understand how they integrate research into operations.

Dr. Boehm-Davis would incorporate the recommended changes to the letter and a revised letter will be sent to the members via email for approval.

Adjourn

Dr. Boehm-Davis thanked the members for attending the meeting and reminded the members the next meeting was scheduled for April 23-24. The meeting was adjourned at 11:40 a.m.

Attachment 1

Research, Engineering and Development Advisory Committee
Holiday Inn Rosslyn Westpark Hotel
1900 North Fort Myer Drive, Arlington, VA 22209
(703) 807-2000   Fax: (703) 522-7480

January 16, 2002

9:00 – 9:30 am	Welcome and Introductory Remarks	Dr. Deborah Boehm-Davis, Chair Mr. Steve Zaidman, FAA Dr. Herman Rediess, FAA
9:30 – 10:15 am	Status Report on Security Subcommittee Report	Mr. John Klinkenberg
10:15 – 10:30 am	BREAK	
10:30 –11:30 am	Committee Discussion on Security Report	Dr. Deborah Boehm-Davis, Chair
11:30 – 12:00 noon	Final Comments/Approval of Security Report	Dr. Deborah Boehm-Davis, Chair
12:00 noon	LUNCH	
1:00 – 2:00 pm	Committee Approval on FY 04 Guidance	Dr. Deborah Boehm-Davis, Chair
2:00 pm	Adjourn	

Attachment 2

Research, Engineering and Development Advisory Committee

January 16, 2002

Attendance

Members

Dr. Deborah Boehm-Davis, Chair
Mr. John Kern
Mr. John O'Brien
Mr. Hans Weber

Mr. Chet Ekstrand
Mr. John Klinkenberg
Mr. John Olcott
Dr. Andres Zellweger

Dr. John Hansman
Dr. Louis Mancini
Mr. Neil Planzer

Audience

Jim White, FAA
Mike Perie, ATCA
John Rekstad, FAA
Paul Polski, FAA
John Panella, USCS
George Marania, FAA
Eric Ransdell, NBAA
Rebecca Ross, BAE
Michael Toscano, OSD
Geoff Mumford, APA
Colin Drury, Univ. of Buffalo
Tony Freck, GE Aircraft Engines
Katherine Yutzey, DOT-OIG
Virgenia Embrey-Brock, FAA
Cymando Henley, CSSI, Inc.
Nick Stoer, Self/NCAR
John Libonati, OWC
April Gessner, CSSI, Inc.

Frank Petroski, MITRE
Amy Zezula, HAI
Mari Peterson, SRI Int'l.
Chris Seher, FAA
Michael Werbowetzki, SEATEK
Dan Smith, FAA
Lyle Malotky, FAA
Tony Vanchieri, FAA
David Evans, Air Safety Week
Jim Jones, FAA
Ed Feddeman, House Science Committee
Terry Kraus, FAA
Stephen Luckey, ALPA
Sharon Hallowell, FAA
Joe DelBalza, JDA
Tammy Jones, FAA
Angelynn Hall, SAMA
Gloria Dunderman, CSSI, Inc.

Herm Rediess, FAA
Lennard Wolfson, DOD
George Skaliotis, VOLPE
Ken Susko, ASF Corp.
Pat Marsha, Galaxy Scientific Corp.
Tom Proeschel, FAA
Karen Stewart, FAA
Paul Busick, FAA
Louis Muniak, CSSI, Inc.
Joseph Hetrick, BAE
Clyde Miller, Northrop Grumman
Curt Boetteher, DOT-OIG
Robert Doll
Don Collier, ATA
Randy Stevens, FAA
Paul Hudson, ACAP
Denise Davis, FAA

Attachment 3

11/16/01

TO: MEMBERS OF FAA'S AD HOC REDAC SECURITY SUBCOMMITTEE ON TECHNOLOGIES AND PROCEDURES TO PREVENT OR MITIGATE AVIATION TERRORISM

FROM: PAUL HUDSON, EXECUTIVE DIRECTOR, AVIATION CONSUMER ACTION PROJECT (ACAP), MEMBER OF FAA AVIATION SECURITY ADVISORY COMMITTEE, THE AD HOC COMMITTEE, AND THE AIRPORT SCREENING CHECKPOINT TEAM

In response to the chair's request for all comments at the November 16th, 2001 meeting of the Ad Hoc Subcommittee, the following are my general comments which I would request be included in the final report as a dissenting view unless adopted by the subcommittee and included in the final report:

A) Procedure.

While the first meeting in October had some good discussion and the process was open and fair. I am somewhat dismayed at the process followed subsequently. As I noted at today's meeting, I was at a disadvantage at today's meeting because no meeting or conference call was ever held by the Airport Screening Checkpoint Team. I was told by FAA that I should not attend the meeting this morning as that was only for the Team Leaders. No draft Team Report was circulated and I first saw the Team Leader's Report at the meeting of the Ad Hoc Committee which began at 1:00 pm. I was also advised team member Colin Drury, Industrial Engineering Professor at SUNY Buffalo, that he also only received a copy of the Team Report this morning. The fourth team member, Dick Doubrava of ATA, did not attend today's meeting, and I received no communication or comments from him. As there were about 350 technical proposals, we should have had a half to full day meeting for each team to evaluate them, rather than have it done "on the fly" as one team leader noted at today's meeting.

At the meeting there were presentations by each Team Leader of his report and time for questions. But no votes or consensus was solicited or reached. The meeting concluded at about 4 pm with the chair simply strolling out of the meeting room. This whole process followed has been fragmented and rather slipshod. Especially if other Teams have followed the same process.

Accordingly, the Airport Screening Team Report at present should be viewed as the product of team leader Nick Cartwright, Director of Transport Canada's EDS Project.

B) Screening Comments.

1) Several of the Team Reports and comments favor the use of ID cards with biologic identification information encoded in them (**smart cards**). The basic problem as noted by John Klinkenberg at the meeting is they are only as good as the methods used to initially establish ID, and there is no real time capability to check names against data bases such as terrorist watch lists.

Accordingly, smart cards must not be issued to passengers, contrary to what is being advocated by some in the airline and security ID industries, because smart terrorists will be able to obtain them and use them to bypass most or all security. We know that the US is faced with smart terrorists who often have good ID , that terrorists and many criminals are adept at identity theft (several of the 9/11 hijackers are reported to have used this method, and the most notorious terrorist now in US custody, Ramzi Youssef, is suspected of having stolen the identity of a British resident), document forgery, and the creation of fictitious identities. Some terrorist cells are known to use credit card fraud as a way to support themselves.

Smart ID cards may have some use with employees, but even here caution is needed in that they should not be used to bypass security (only for additional security), since as one participant at the meeting noted they may go over to the "dark side." At present, there are reported to be over 40 pilots on the FBI terrorist wanted list, and US based terrorists have been discovered with airport ID that would allow them access to airliners. After 9/11 box cutters were reported discovered on several airliners flying out of Logan Airport. Employee corruption, smuggling, theft and other criminal conduct is a known problem at a number of large US airports.

The 19 Sept.11th hijackers are reported to have had generally clean criminal history records, to be foreigners from the Middle East (16 from Saudi Arabia, others from Tunisia, Egypt, all US allies), radical Moslem men, eight with pilot training, between the ages of 21 and 34, and all with US State Department Visas, and passports. Some had US driver's licenses, Social Security Cards, pilot licenses, frequent flyer cards and bank cards. The reported leader also had a graduate degree in city planning. And an associate of the 9/11 terrorists arrested in Britain is reported to be a commercial pilot.

Other master terrorists have often had engineering backgrounds, some like the Pan Am 103 terrorists were foreign airline security personnel, others like the Air India bombers were respected businessmen (Sikhs who were long time Vancouver, Canada residents), or decorated ex US military personnel (e.g. Timothy McVeigh). Barring some very legally questionable profiling and discrimination based on national origin, religion, age, sex, educational background, etc., the typical smart aviation terrorist of today would qualify for and probably obtain a smart ID card to avoid airport security checks, if they were made available.

The argument that we need to pre-clear a large group of passengers (one meeting participant suggested 50 million) so we can concentrate on a smaller group of non-cleared passengers is specious, because the history of aviation security indicates this does not occur, for cost and commercial convenience reasons. Moreover, the risk of giving smart terrorists little or no security checks is far too great.

Finally, a smart card issued to certain frequent flyers is reverse or positive profiling, and profiling has generally been a failure in aviation security, particularly when used for anti-hijacking security. Prior to 1970 the anti-hijacking profiling system then in place was completely ineffective to prevent nearly one hijacking per week, versus the success of universal security screening with X-rays and metal detectors that deterred or prevented most US domestic airliner hijackings as soon as the system was installed.. The failure of CAPPS to stop any of the 19 Sept. 11th hijackers should give pause to anyone even contemplating such systems to be anything more than an auxiliary to a universal security system. Profiling also failed in the case of the Unabomber even after six years of serial bombings.

2) A **universal, in depth screening system** should be used in the future. Such a system could have the following features: a) A second screening of 10% of all passengers/carry ons on a random basis, plus selectees (at least another 10%) (this would provide continuous quality control for the main screening checkpoints and would quickly weed out incompetent or tired or impaired screeners); b) hand searches of all passengers meeting selectee criteria plus a random group, plus hand searches of their carry on baggage; c) questioning of a selection of passengers (at least 5%) most of whom would be advised in advance to report early for security checks. Last week the fact that a second search was done at the gate in Chicago prevented a passenger from carrying on board 7 knives, a stun gun and a can of pepper spray in his carry on bag.

Other universal security systems that should be studied to see how their high security operates in areas open to the general public, include casinos, banks in most foreign countries, embassies, national art museums, Swiss and Israeli aviation security, as well as facilities with more limited access such US military installations with weapons of mass destruction, the US Mints and Federal Reserve Banks.

3) **Reduction of carry-on luggage** to levels at which screening check points can reliably detect at least 95% of prohibited items should be required immediately to mitigate against the risk of more airliner hijacking. Reductions to date are not sufficient.

4) **Frequent testing of screening** check points with red teams and with test object **exercises**, as well as proficiency **testing** is vital to maintaining high standards of competence, readiness and alertness. Screening personnel need to be rewarded for superior performance and penalized for inferior performance. Also competition between screening teams, and esprit de corps needs to be fostered. These methods and especially war games are used by the military, to maintain and improve readiness and efficiency, and should be adopted for screeners. Unlike law enforcement officers or even most security guards who often face criminal situations, most screeners will never come face to face with a terrorist. Only with testing and anti-terrorist gaming methods can we expect screeners and their supervisors to reach and maintain a high level of competence and alertness. The current system lacks these features and fosters boredom, constant small

talk and social chit chat among screeners, and a general lack of seriousness and competence, all of which is noticed by passengers and undermines public confidence in air travel security.

C. Aircraft Hold Areas and Cabin Supplies.

1) Purchase and use of **hardened cargo and baggage containers** should be added to this report. This technology has been well tested and is ready for deployment. Its deployment would mitigate or prevent airliner bombing to a large degree, especially if coupled with check baggage and cargo screening.

2) As small bombs placed over the center fuel tank is a known method of aviation bombers (e.g. 1989 Avianca bombing, Columbia; planned Ramzi Youssef bombing 11 US airliners in the Far East), **center fuel tanks should be inerted**. This measure would also prevent accidental explosions of these tanks as happened in 1996 with TWA 800 and earlier this year in the Far East. The FAA is presently considering such a measure, and it has been studied at length by two industry task forces (in 1998 and 2001) who both found it to be technically feasible. It is presently pending before the executive committee of the FAA Aviation Rulemaking Advisory Committee (ARAC). This is also mature technology that has been used in military aircraft for decades. ACAP originally petitioned the FAA to mandate this technology in the mid 1980's.

3) **Banning of unscreened mail and cargo** over 12 ounces unless contained in a bomb resistant container on all passenger airliners. The ban was instituted during the Gulf War and was in place from Sept. 12 to 17th, 2001, when it was replaced with enhanced know your shipper regulations. The current FAA policy is inadequate to prevent a massive airliner bombing attack. Technology for screening cargo is available and needs to deployed if airliners are to safely carry mail and cargo over a certain weight known to be sufficient to bring down an airliner with a bomb. Anyone familiar with the current air cargo or mail system could plant multiple bombs on US airliners. The Unabomber threatened and had the capacity to carry out such attacks, no doubt others do also.

D. Forward Looking Issues Team Report

1) This report omits the most serious future attack possibilities and vulnerabilities, including:

-Use of **small aircraft to spread biological or chemical aerosols in urban areas**, with the potential for killing several hundred thousand to several million. This is in my view the most likely means for terrorists to top the 9/11 attacks. We know they were planning or considering such attacks and we have already been attacked by weaponized anthrax in the mail. It has also been reported that hundreds and perhaps thousands of young men from Middle Eastern countries have received pilot training at US flight schools (ads for these flight schools have recently been discovered in bin Laden terrorist facilities in Afghanistan). News reports have said that 44 pilots are on the FBI terrorist suspect list.

According to the Johns Hopkins Biodefense web site (citing US Congress Office of Technology Assessment and UN agency analyses, and referenced by the CDC) 50 kilograms of aerosolized anthrax (1 gram contains a reported 1 billion spores), as has already been used against the US Government and media, spread by a small aircraft for less than a mile could be expected to create a deadly aerosol that would kill 100,000 to 3 million in a metro area of 5 million. As there are presently no detectors, we would not know an attack occurred until the people fell ill with inhalation anthrax, which is often to usually fatal. In sum, we know terrorists have these weapons and that our defenses are inadequate to nonexistent, and that they are capable of obtaining and using small civilian aircraft in the US. What we do not know is how much they have and whether it will soon be dispersed by aircraft or some other means.

-Use of **larger non-airliner civilian aircraft to crash into US landmarks, nuclear facilities or mass gatherings.**

Nuclear power plants are vulnerable to attack by air especially the control buildings and spent fuel storage pools that are do not have a containment structures to protect them. A typical nuclear power plant contains about 1,000 times the radioactive material of a Hiroshima size bomb, so even a 1% release to the atmosphere could do enormous damage.

The security on non-airliners in the US is minimal to nonexistent. The main security currently is the US Air Force, which is spread much too thin for good air cover protection over likely targets.

-Use of **civilian aircraft to deliver nuclear or radiation bombs** over US cities.
A present overt threat has been made by the bin Laden terrorists and the Taliban leader backed up by some intelligence reports; the nation's top leaders say it cannot be completely discounted.
A nuclear device would probably do the most damage to the widest area if exploded in the air over or near a major city.

-Use of **large (tractor trailer trucks) with fertilizer bombs to wipe out airports** or other ground targets up to several square blocks. The use of truck bombs is presently the third most deadly form of terrorism actually used, we know now that some suspected terrorists in the US have obtained commercial trucking and even hazardous materials licenses which would allow far more powerful bombs to be used.

-Use of **Stinger missiles against airliners on take off or landing**.
Hundreds of such weapons are reported to be on the black market or in the hands of terrorists.

-Use of **foreign commercial airline pilots flying jumbo jets in the US for suicide attacks on US targets.** The EgyptAir crash could be a preview of something far more sinister and serious.

All of the above scenarios could result in thousands to millions of deaths and injuries, some could make certain urban areas uninhabitable for many years, and all would cause the US and probably the world economy to go into a deep recession..

Of the scenarios mentioned in the Report most are backward looking and most have in my view about as much chance of occurring as a 1960s or 1970s style hijacking for publicity or shock value. Terrorists tend to want each act to match or exceed the ones before it, otherwise it will not shock or terrorize the population.

2) The **bin Laden terrorists are clear in their objectives**: They want to kill as many Americans as possible (thousands to millions), destroy the US infrastructure, show the world, and especially terrorist groups and the Islamic world, that the US is a paper tiger that cannot effectively defend its homeland against such attacks, provoke a general war between Moslems and the West, and intimidate, de-legitimize, and/or kill off moderate or secular Moslem forces and governments. Their announced goals are to force US military withdrawal from the Middle East (especially Saudi Arabia) and other Islamic countries (making their governments ripe for overthrow by radical Islamic forces) and an end US support of Israel and the state of Israel. Ultimately the Bin Laden terrorists envision a caliphate or a Moslem superstate. As implausible as these goals sound, the history of 20th Century fascism and communism shows that they are not impossible. Especially if they are right in their basic assertion that the US is highly vulnerable at home and incapable of defending itself against terrorist infiltration and attack.

Unlike other terrorists of the 20th Century, the bin Laden terrorist network is very well organized and financed with an organizations in about 60 countries, its members are willing to commit suicide in their attacks, and have a religion based sophisticated, committed and well educated leadership dedicated to mass violence. They are willing to spend years living in, planning for and waiting to attack in the US and other Western democracies on command. These terrorists have shown a particular affinity for aviation terrorism in the US, in both their actions on 9/11 and their threats since then and their activities prior thereto.

3) The **way to mitigate against these threats** is to restrict general aviation and cargo flights near urban areas until security measures are in place to identify both aircraft and pilots as friendly, to deploy detectors or use targeted geographic testing to detect biological and chemical attacks when they occur, to update and test evacuation and other civil defense plans for major cities, to stockpile antidotes and protective devices for known forms of biological, chemical or nuclear attack for the general population with necessary public health resources , to provide for public education to prepare and protect the public from such attacks and avoid panic, and to provide military air cover over likely target areas.

Such measures in peacetime seem inconvenient, expensive and unnecessary, but in wartime, such measures are not only appropriate but may well make the difference between victory and defeat in the war between the US and international terrorist organizations and their supporters. The US faces a global war against elusive decentralized terrorist organizations with a multimillion dollar and person support structure, and several thousand terrorists, coupled with the need to defend against civilian targets both at home and abroad. This is unprecedented in our history and will require both strong offensive and strong defensive measures.

The underlying presumption in the report is that the US is at peace and is faced with some bothersome terrorist threats and the remote possibility of more serious threats in the future is obsolete in light of the Sept. 11th Attacks and subsequent events. We must presume that terrorist threats of mass destruction and more aviation terrorism are likely and plan accordingly.

The old approach of discounting more serious attacks as too unlikely to seriously plan for must be discarded. The usual calculus of multiplying the likely damage times the likely risk of occurrence must be updated at the very least to increase the likelihood of major attacks on the US homeland by terrorists and also to increase the range of uncertainty in our estimates of the probabilities. The Government should not heavily rely on the opinions of terrorist experts as their prediction track record is very poor. War is inherently uncertain. The public has entrusted the Government fight and win wars and protect the national security. They will follow Government leadership and put up with almost any inconvenience, but dishonesty, incompetence or wrongheaded predictions and false reassurances. To protect your credibility, eschew predictions. Leave predictions to the pundits, idle ex officials, and experts whose predictions will more often be wrong than right.

Likewise the tombstone approach of never acting until after the disaster has occurred can no longer be tolerated. What will the Government say to the American people the day after a biological or nuclear 9/11 attack? The answer that our experts did not think it was likely so we did nothing to plan for or defend against it will not be tolerated. Rather the new approach must be to plan for and defend against more serious attacks in anticipation that they will be attempted in the future, unless there are very strong defensive or deterrent measures in place. No new form of terrorism has not been repeated without strong defensive or deterrent measures in place. Deterrence against terrorist organizations has been nearly nonexistent, unlike terrorist nations that cannot hide once they are identified.

We must also assume that some attacks cannot be prevented and have contingency plans in place for civil defense measures to mitigate the physical, economic and psychological damage of such attacks. Such plans were in place in varying degrees during the Cold War and World War II.

Where priorities are necessary due to limited resources, in my view the focus should be on defending against major threats (those that would kill thousands or millions or destroy national symbols or Government command and control centers), rather than defending against minor threats (those that would kill hundreds or less).

Unfortunately, the Forward Looking Issues report essentially ignores the major threats and would have the Government's resources devoted to prevention of minor threats. This approach in my view is very poor tactics and use of limited resources.